

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
Wireless Telecommunications Bureau
Amateur Radio Service
Via the Electronic Comment Filing System
445 12th Street SW
Washington, D.C. 20554

In the Matter of)	
)	
Response to Request for Rule Making)	RM-11699
)	Encryption of Amateur Radio Communications

Glenn B. Schulz, W9IQ
20585 W. Good Hope Road
Lannon, WI 53046

Respondent

July 4, 2013

Respondent Qualifications

By way of background, I am an Amateur Radio Extra Class licensee, W9IQ and a Lifetime FCC General Radio Telephone licensee with ship radar endorsement, PG-18-24500. I hold various FEMA disaster management certifications including FEMA 100 and FEMA 700. I have served as an Assistant Emergency Coordinator for the American Radio Relay League (ARRL) Amateur Radio Emergency Services (ARES®) organization in the role of developing and maintaining emergency communications infrastructure.

Professionally I am a certified expert in cryptography (ISSAP # 53380) holding United States and international patents in the domains of firewalls, authentication, and encryption as well as a Certified Information Systems Security Professional (CISSP # 53380). I have acted as a liaison and consultant to the Department of Homeland Security in the area of critical infrastructure protection in the domains of industrial control networks and systems.

Executive Summary

RM-11699 asks that the Amateur Radio Service be granted the authority to use encryption for emergency communications and related drills. This respondent believes that the basis for this request is fallacious in that no statutory or durable practical requirement for encryption exists under the petitioners described circumstances.

While the Amateur Radio operators may not generally obscure the meaning of a message, the regulations¹ already tacitly permit encrypted communications in emergency situations: "No provision of these rules prevents the use by an amateur station of any means of radiocommunication at its disposal to provide essential communication needs in connection with the immediate safety of human life and immediate protection of property when normal communication systems are not available."

In the event other unforeseen circumstances arise in which the Amateur Radio Service needs to provide encrypted communications, the FCC has the authority to issue emergency orders or temporary station authorizations to address such needs prior to taking a more durable regulatory approach.

The ubiquitous use of encryption by the general public due to the need for data security on wireless networks and the Internet has left some Amateur Radio licensees to suggest that it is "OK" to use

¹ CFR Title 47 Part 97.403

encryption in the Amateur Radio Service. Even a popular Amateur Radio magazine published an article² suggesting that encryption is legal for the Amateur Service. The apparently flawed logic of confusing authentication and encryption has permeated the Amateur Radio community.

This respondent respectfully requests that RM-11699 be dismissed without prejudice; that the FCC in its ruling clarify the synonymous meaning of "encryption" and the part 97 prohibition of "obscuring the meaning"; and that the FCC confirm that encryption would be permissible when required only under the limited scope of CFR Title 47 Part 97.403.

General Discussion

Encryption and Part 97

It is helpful to establish some standard of terminologies related to encryption that originate in the field of cryptography:

Encryption: The process of disguising a message so as to obscure its content and substance.

Cleartext: A message whose content and substance is not obscured.

Ciphertext: An message that is obscured through encryption.

Decryption: The process of converting a ciphertext message to a cleartext message.

It should be noted that some organizations use the term enciphering and deciphering to denote encryption and decryption, respectively.

Encryption and decryption can be accomplished through the use of restricted (secret) algorithms or through well published algorithms. Published algorithms favor the use of keys within the encryption or decryption algorithms. Restricted algorithms may use keys or simply rely on the secrecy of the algorithm.

Conventional cryptographic terms are not used in Part 97 regulations that govern the Amateur Radio Service but rather the regulations use the term "obscure" or "obscuring". The regulations³ prohibit "... messages encoded for the purpose of obscuring their meaning.." with exceptions for specified

² "Data Encryption is Legal!" by Don Rotolo, N2RIZ, CQ Magazine, August 2006 <http://hsmm-mesh.org/images/stories/DataEncryptionIsLegal.pdf>, accessed 3 July 2013

³ CFR Title 47 Part 97.113(a)(4)

telecommand and telemetry applications. Further the regulations⁴ permit the use of published digital transmission modes provided that "... using unspecified digital codes must not be transmitted for the purpose of obscuring the meaning...". The regulations⁵ also permit the limited use of spread spectrum transmission provided that they "must not be used for the purpose of obscuring the meaning of any communication."

When one considers that encryption obscures the content and substance of the message and that the Amateur Radio regulations repeatedly prohibit the obscuring of the meaning of a transmission, it becomes clear that the use of encryption is not permitted in the Amateur Radio Service except for described telecommand and telemetry purposes. It then follows that it does not matter whether the encryption is accomplished through restricted or published algorithms, keys or keyless systems - the prohibition applies to all methods and algorithms of encryption.

Some proponents of encryption have argued that encryption is necessary to keep non Amateur Radio licensees off of certain Amateur Radio Services and infrastructure. This is a technically flawed argument that is addressed in the later [Amateur Radio 802.11 and Encryption](#) section.

HIPPA and Radio Encryption

Proponents of the need for encryption in the Amateur Radio Service often cite the data security requirements specified in HIPPA privacy rule regulations⁶ and erroneously express that Amateur Radio transmissions must be encrypted when carrying out communications for an entity regulated by HIPPA regulations.

It should be noted that the privacy rule regulations⁷ describe all uses of encryption as "Addressable" and not "Required". Furthermore the Office for Civil Rights (OCR), the division of the Department of Health and Human Services responsible for enforcing the HIPPA privacy rule, has issued explicit guidance⁸ stating "... the Privacy Rule does not require the following types of structural or systems changes:... encryption of wireless or other emergency medical radio communications which can be intercepted by scanners."

⁴ CFR Title 47 Part 97.309(b)

⁵ CFR Title 47 Part 97.311(a)

⁶ CFR Title 45 Part 164, "Security and Privacy"

⁷ CFR Title 45 164.306(d)1

⁸ <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalu&d.pdf>, accessed 2 July 2013

This explicit exemption to changes for encryption of wireless communications clearly applies to all radio communications carried out by Amateur Radio operators when serving HIPPA covered entities or transmitting HIPPA covered information under any circumstances, including emergency situations and drills.

Amateur Radio 802.11 and Encryption

Proponents of the need for encryption in the Amateur Radio Service often cite the need to use encryption to keep non-licensed stations from accessing 802.11 (Wi-Fi) devices operating in the 13 cm band that have been repurposed for the Amateur Service through the use of gain antennas or increased transmission power. This claim is ill-founded since encryption does not exclude non Amateur Radio licensees from accessing these stations but rather it is authentication and authorization that is required to achieve this goal.

Authentication is the ability of one party to positively confirm the identity of another party.

Authentication can be accomplished through well published and accepted protocols that apply cryptographic techniques without the use of encryption. The messages exchanged during authentication are structured, cleartext messages whose purpose is not to "obscure the meaning of the message" as described in Part 97.

Other cryptographic techniques and standards that enhance the service level of messages and do not involve encryption are available to the Amateur Radio Service:

- Integrity: The ability of a receiver of a message to verify that the message has not been modified in transit.
- Nonrepudiation: The inability of a sender to falsely deny that he sent a particular message.

Amateur Radio Interoperability

The established nature of the Amateur Radio Service is that all methods of modulation and signal encoding are well-known well published and widely understood within the Amateur Radio Service . This provides an inherent level of interoperability. No licensee is excluded due to incompatibility of technologies or methodologies. This broadly woven interoperability is responsible in no small way for the ability of the Amateur Radio Service to carry out communications in a wide variety of emergency situations.

In contemplating the use of cryptography in the Amateur Radio Service, due consideration must be given to the potential loss of interoperability among all Amateur Radio Service operators. Any protocol or methodology that excludes or limits an Amateur Radio operator from participating in the communication chain necessarily degrades the potential of the Amateur Radio Service to carry out the desired communications.

Any encryption protocol, methodology, or key that is exclusively known or used by one organization of Amateur Radio operators will effectively isolate all other Amateur Radio operators having the potential of forming clubs, organizations, classes and cliques that can detrimentally fragment the Amateur Radio community.

Amateur Radio Regulatory Enforcement and Self-Policing

The fraternal nature of the Amateur Radio Service has long fostered an environment of self-policing that relies on the ability of Amateur Radio operators to monitor the method, quality, and content of the transmissions of other Amateur Radio operators. This activity has also been formalized through the American Radio Relay League and the Amateur Auxiliary⁹ program consisting of 700 volunteer appointees carrying out roles as Official Observers and members of the License Interference Committee. In cases involving serious rule violations, such as malicious interference, they are trained and certified to gather and forward evidence that can be used by the FCC in enforcement actions. The program is based on a formal agreement between the FCC and the ARRL.

Any consideration for the use of encryption in the Amateur Service must examine its effects on this well organized self-policing model and on the ability of the FCC and other governmental agencies to carry out necessary enforcement actions related to transmissions in the Amateur Radio Service.

International Conventions

Any consideration for the use of encryption in the Amateur Radio Service must also take into account international conventions to which the USA is a party. For example, ITU regulations¹⁰ reflect the wording of the current Part 97 FCC regulations: "Transmissions between amateur stations of different countries shall not be encoded for the purpose of obscuring their meaning..."

⁹ <http://www.arrl.org/amateur-auxiliary>, accessed 3 July 2013

¹⁰ ITU Article 25, Section 1, Paragraph 25.2a

Practical Approaches to Encryption in the Amateur Radio Service

Should the FCC find that encryption in the Amateur Radio Service is necessary or desired, methods do exist whereby the entire Amateur Radio community could participate in handling messages encrypted for served agencies without hindering the enforcement of the Amateur Radio Service regulations. Regardless of the method employed, care must be taken to ensure that the necessary station identifiers are transmitted in cleartext.

Encryption by the Served Agency

The FCC could grant the ability for the Amateur Radio Service to transmit messages encrypted and decrypted directly by the served agency in times of emergencies and drills. By specifying the conditions under which such encrypted messages can be passed and by describing the scope of served agencies, the general proliferation of encryption by the Amateur Radio Service can be avoided. Since the message from the served agency would be presented to the Amateur Radio operator in the form of ciphertext, the FCC would need to amend the statutory responsibility of the Amateur Radio operator regarding the content of the message.

The primary limitation of this approach is that not all agencies that require encryption may have encryption protocols and methodologies defined or available for ad-hoc radio communications such as what would exist in the time of emergency.

Consideration must also be given to the potential of an Amateur Radio operator becoming an unwitting participant in nefarious or illegal activities.

Community Keys

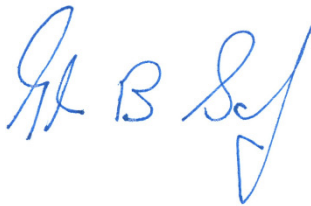
The FCC could permit an encryption system whereby all Amateur Radio operators and necessary government enforcement agencies have unrestricted access to the necessary algorithms and keys for any approved use of encryption. Such an approach would allow amateurs to meet existing regulations regarding origins and content of messages; allow all willing and available Amateur Radio operators to participate in the encrypted communications as appropriate; and to not hinder any voluntary policing or government enforcement of the Amateur Radio regulations.

The strength of modern key based encryption algorithms relies heavily on the secrecy of the private keys. Distributing and managing keys for licensed Amateur Radio operators could be accomplished on a

wide scale as has been demonstrated by the PKI (Public Key Infrastructure) with robust authentication as established by the American Radio Relay League for its Log Book of the World program¹¹.

The FCC could also adopt companion regulations that prohibit others from decrypting messages encrypted by this service as well as prohibiting the unauthorized use, distribution, and disclosure of private keys associated with the service.

Respectfully Submitted,

A handwritten signature in blue ink, appearing to read "Glenn B. Schulz". The signature is stylized with a large "G", a small "B", and a large "S" followed by a checkmark-like flourish.

Glenn B. Schulz, W9IQ
20585 W. Good Hope Road
Lannon, WI 53046

¹¹ <http://www.arrl.org/logbook-of-the-world>, accessed 3 July 2013